METHOD AND DEVICE FOR AUDITING COMMUNICATION DATA

Patent Number: JP10111855
Publication date: 1998-04-28
Inventor(s): DOMYO SEIICHI;; SATO MAKOTO;; TAKARAGI KAZUO;; NANBA AKIRA
Applicant(s): HITACHI LTD
Requested Patent: JP10111855
Application Number: JP19960264051 19961004
Priority Number(s):
IPC Classification: G06F15/00; G06F13/00; G09C1/00
EC Classification:
Equivalents:

Abstract

PROBLEM TO BE SOLVED: To keep communication data secret by detecting the secrecy level of a computer or network on the basis of a label, and recording a face photograph of an operator or operation screens of respective computers as a history when the communication data are accessed or copied.
SOLUTION: The communication data with the attached label are downloaded through a firewall (S110) and the label in certain format is extracted (S111). If the label can not be extracted (S112), error processes following S140 are performed. The contents of the label, e.g. a kind indicating secrecy and a usable range are read out and on the basis of a digital signature given as well as ciphering, it is decided whether or not the label is forged (S114). Further, the secrecy level is decided on the basis of the label (S116). Specially, when a decision can not be made by a local machine, a label inspection server on the network is inquired to retrieve the relation between the described label and secrecy level (S115, S130, and S131).

通信データ監査方法および装置

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平10－111855

(43)公開日　平成10年(1998)４月28日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ	15/00	３３０Ｚ
	13/00	３５１		13/00	３５１Ｚ
Ｇ０９Ｃ	1/00	６６０	Ｇ０９Ｃ	1/00	６６０Ｅ

審査請求　未請求　請求項の数９　ＯＬ　（全 13 頁）

(21)出願番号　特願平8－264051

(22)出願日　平成８年(1996)10月４日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　道明　賦一
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(72)発明者　佐藤　真
東京都江東区新砂一丁目６番27号株式会社日立製作所公共情報事業部内

(72)発明者　宝木　和夫
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

最終頁に続く

(54)【発明の名称】　通信データ監査方法および装置

(57)【要約】

【課題】イントラネットのシステム管理者は、コンテンツをイントラネット内で流通させるにあたり、以下の課題をもつ。

(1) 契約外コンテンツの無断流通の抑制

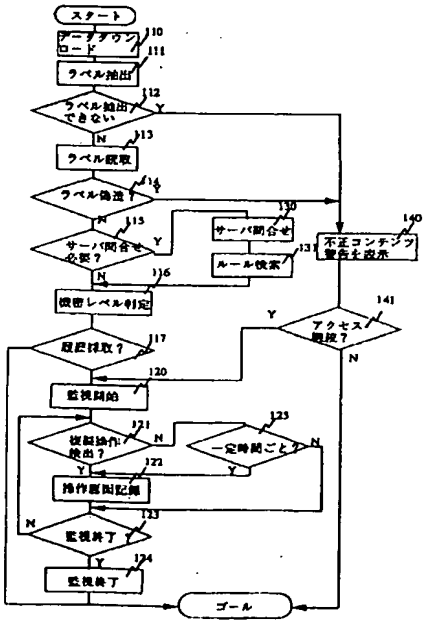
(2) コンテンツの無断複製行為の抑制

【解決手段】(1) 企業独自のラベルを設け、ネットワーク内のコンテンツ流通を制御する。

(2) コンテンツ複製の操作画面ならびに利用者の顔写真を履歴として記録する。

(3) とくに、(1)のラベルの種類に応じ、(2)の履歴を記録する方法や管理形態を決定する。

図 1



【特許請求の範囲】

【請求項１】ネットワークに複数の計算機を接続し、前記計算機の相互間で、通信データならびに前記通信データに関するラベルを転送し前記ラベルを参照し、前記通信データの機密レベルを判定する計算機の通信データ監査方法において、

前記ラベルをもとに、前記計算機あるいは前記ネットワークの範囲で有効な機密レベルを検出するステップと、通信データをアクセスあるいは複製するステップと、操作者の顔写真あるいは各計算機の操作画面を履歴として記録するステップとを含むことを特徴とする通信データ監査方法。

【請求項２】異なる機密レベルを設定したネットワーク間を流れる通信データを一時的に蓄積するファイアウォールであって、機密レベルの高いネットワークに接続する計算機が、通信データ蓄積装置として利用するファイアウォールにおいて、

機密レベルの低いネットワークから受信した通信データに機密レベルの属性を示すラベルを添付する手段と、機密レベルの低いネットワークに送信する通信データから前記ラベルを削除する手段を有することを特徴とするファイアウォール。

【請求項３】複数の計算機と監査装置とをネットワークで接続し、前記計算機での通信データのアクセスおよび複製の操作履歴を監査者に提示する通信データ監査装置において、監査者の公開鍵を生成し、前記計算機に送信する鍵生成手段と、操作者の顔写真および画面内容の暗号化した操作履歴を蓄積する履歴蓄積手段と、監査者の秘密鍵で操作履歴を復号する履歴復号手段とで構成することを特徴とする通信データ監査装置。

【請求項４】複数の計算機と監視装置とをネットワークで接続し、前記計算機での通信データのアクセスおよび複製の操作履歴を監視する通信データ監視装置において、通信データに添付された機密ラベルと、監査規則の対応表を記録する規則設定手段と各計算機の問い合わせに応じて、上記対応表を検索し、上記通信データに関する履歴採取の必要の有無を返信する機密判定手段とで構成することを特徴とする通信データ監視装置。

【請求項５】請求項１において、機密レベルを示すラベルが未検出の際に、計算機の操作画面に通信データのアクセス禁止を示す勧告メッセージを表示するステップを有する通信データ監査方法。

【請求項６】請求項１において、利用者あるいは計算機ごとに独立した暗号鍵で、ラベルならびに通信データを復号するステップを有する通信データ監査方法。

【請求項７】請求項２において、機密レベルの低いネットワークの計算機から送られた通信データを蓄積する手段であって、機密レベルの高いネットワークの少なくとも一つの計算機および少なくとも一人の利用者が復号できる暗号化鍵を保有し、通信データとラベルを結合したデータを、前記暗号化鍵を用いて暗号化し、ラベルを暗号化するラベル添付手段を含むファイアウォール。

【請求項８】請求項２において、機密レベルの高いネットワークの計算機から送られた暗号化データを蓄積する手段であって、上記暗号化データを復号する復号鍵を所有し、通信データとラベルが含まれる暗号データを、前記復号鍵を用いて復号し、前記通信データと前記ラベルとを分離するラベル削除手段と前記通信データを機密レベルの低いネットワークへ送る履歴を機密レベルに応じて蓄積する手段を含むファイアウォール。

【請求項９】複数の計算機とファイアウォールとをネットワークで接続し、

通信データとラベルを受信する計算機に接続する可搬型カードであって、暗号化された前記通信データとラベルを復号する際に用いる可搬型カードで、利用者ならび機密レベルごとに独立し、ファイアウォールとのセッションで生成した暗号鍵を蓄積する可搬型カード。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンピュータネットワークにおける通信データの機密性を確保する技術に関する。

【０００２】

【従来の技術】インタネットおよびイントラネットの普及にともない、いわゆるマルチメディアデータやソフトウエア等のプログラム（以下、コンテンツと記す）をネットワークを介して流通させる上で、以下の問題点が生じている。

【０００３】(1) 不特定多数の利用者によるコンテンツ複製

流通の末端である計算機（パーソナルコンピュータ）で、コンテンツの複製が容易にできる。しかも、権利者が末端のＰＣの状況を監視できないので、知的財産権を主張しづらい。

【０００４】(2) コンテンツの利用時に発生する課金

権利者がネットワークを介してコンテンツを送った段階ではなく、利用者がコンテンツを使用して、初めて対価を権利者に支払う後金方式である。しかし、問題点(1)同様に、権利者が末端の状況を監視できないので、利用者に課金を請求しづらい。

【０００５】このような問題に対処するため、権利者は、自らの情報を電子的なラベルとして添付したコンテンツをネットワークに流通させ、利用者は、コンテンツの使用量に応じ、ラベルに記された権利者に対価を支払う超流通という方式および装置が考案された。超流通は、たとえば森亮一、河原正治、大瀧保広「超流通：知的財産権処理のための電子技術」、情報処理学会，Vol. 37, No. 2, February, 1996で開示されている。

【０００６】

【発明が解決しようとする課題】しかし、上記公知例に

は、イントラネットの設備者（企業）とシステム管理者にとって、以下の不満足な点がある。

【０００７】(1) コンテンツの無断流通を抑制できないシステム管理者は、たとえば、ＣＤ－ＲＯＭやＤＶＤの可搬媒体を用いたインストールする、あるいは、ＦＴＰやWWW等の通信プログラムを用いてダウンロードし、コンテンツを蓄積するサーバ装置を用意する。一般利用者は、サーバ装置にアクセスすることで、コンテンツを利用できる。

【０００８】しかし、一般利用者が、システム管理者に無断でコンテンツを導入し、ネットワーク内で流通させる可能性がある。

【０００９】その際に、計画外のコンテンツの導入により、ハードディスクやネットワーク等の計算機資源を浪費し、業務を阻害するケースが発生する。あるいは、ウィルスがネットワークに混入し、データ破損の経済的被害が発生するケースもありうる。

【００１０】システム管理者は、ネットワーク内で、利用者がコンテンツを無断に流通していないことを設備者に証明する必要がある。

【００１１】(2)コンテンツの無断複製行為を抑制できない

権利者と企業の間で、企業内ネットワークに接続した計算機の使用に限り、コンテンツの複製を許すサイトライセンス契約を結ぶ。権利者は、コンテンツの対価が企業から確実に得られる。企業は、一括して契約を結ぶことで、使用料やコンテンツ管理の手間を削減できる。

【００１２】しかし、一般利用者が、システム管理者や権利者に無断でコンテンツを複製し、契約外のネットワークや計算機で利用する可能性がある。その際に、不正が発覚した場合、権利者が契約違反として企業を訴えるケースが生ずる。

【００１３】システム管理者は、ネットワーク内で、利用者がコンテンツを無断に複製していないことを権利者に証明する必要がある。

【００１４】

【課題を解決するための手段】上記目的を達成するために、ラベルをもとに、計算機あるいはネットワークの範囲で有効な機密レベルを検出し、通信データをアクセスあるいは複製した際に、操作者の顔写真あるいは各計算機の操作画面を履歴として記録する。

【００１５】とくに、機密ラベルの検出にあたり、

（１）機密ラベルが未検出の際に、計算機の操作画面に通信データのアクセス禁止を示す勧告メッセージを表示する。

【００１６】（２）ファイアウォール等で暗号化されたラベルを、利用者あるいは計算機ごとに独立した暗号鍵で復号する。

【００１７】であると望ましい。

【００１８】監査用装置をネットワーク上に設ける。

【００１９】この監査用装置は、監査者の公開鍵を生成し、計算機に送信する鍵生成手段と、監査者の公開鍵を用いて暗号化した各計算機の履歴を蓄積する履歴蓄積手段と監査者の秘密鍵で操作履歴を復号する履歴復号手段とで構成する装置が望ましい。

【００２０】監視用装置をネットワーク上に設ける。

【００２１】この監視用装置は、通信データに添付された機密性を示すラベルと監査規則との対応表を記録する規則設定手段と、計算機の問い合わせに応じて、対応表を検索し、通信データに関する履歴採取の必要性の有無を返信する機密判定手段とで構成する装置が望ましい。

【００２２】また、上述したラベル制御を前提とするネットワークに設置するファイアウォールは、機密レベルの低いネットワークから受信した通信データに機密レベルの属性を示すラベルを添付する手段と、機密レベルの低いネットワークに送信する通信データから上記ラベルを削除する手段を有することを特徴とする。

【００２３】とくに、

（１）機密レベルの高いネットワークの少なくとも一つの計算機および少なくとも一人以上の利用者が復号できる暗号化鍵を保有し、通信データとラベルを結合したデータを、上記暗号化鍵を用いて暗号化し、ラベルを暗号化する。

【００２４】（２）暗号化データを復号する復号鍵を所有し、通信データとラベルが含まれる暗号データを、復号鍵を用いて復号し、通信データとラベルとを分離するラベル削除し、通信データを機密レベルの低いネットワークへ送る履歴を機密レベルに応じて蓄積する。

【００２５】であると望ましい。

【００２６】また、ラベル復号用の可搬型カードを各計算機で利用する。

【００２７】この可搬型カードには、利用者ならび機密レベル別に独立した暗号鍵を蓄積し、ファイアウオールで暗号化したラベルならび通信データを復号する際に用いるのが望ましい。

【００２８】

【発明の実施の形態】本発明の実施例を図面を用いてより詳細に述べる。

【００２９】図１は、本発明を施した、計算機におけるコンテンツ監査方法の流れ図である。

【００３０】図１で、１１１はコンテンツよりラベルを抽出する処理、１１６は抽出したラベルをもとにコンテンツの機密レベルを判定する処理、１２１は、利用者のコンテンツの複製操作を検出する処理、１２２は操作画面を記録する処理である。機密レベルに応じて履歴（操作画面や利用者の顔写真）を記録するかどうかを判定するところに特徴がある。

【００３１】図２は、本発明のラベルを添付するファイルアウォールの１実施例を示したブロック図である。

【００３２】図2において、２３１はラベルを添付する

プログラム、２３２はラベルとともに通信データを暗号化するプログラム、２４１はラベルを破棄するプログラム、２４２はラベルを復号するプログラムである。ファイルアウォール２１０は、機密レベルの異なるネットワークに接続し、低いレベルのネットワークから送られた通信データを暗号化し、高いレベルのネットワークから送られた通信データを復号するところに特徴がある。

【００３３】図３は、本発明で記録した操作履歴を暗号化し、監査者用のサーバに送信し、蓄積する構成を示したブロック図である。この例は、暗号鍵と復号鍵が異なる非対称暗号方式を用いた実施例である。

【００３４】図３で、３６１は（監査者の公開鍵３２１と秘密鍵３２２を生成し）、公開鍵３２１を履歴を記録する各計算機に配布する鍵（生成）配布プログラムである。３６２は各計算機の操作履歴３２４を蓄積するプログラム、３６３は操作履歴３２４を復号し、監査者に提示するプログラムである。図３では、各計算機で暗号化し、監査者サーバに送ることで、業務の機密も守り、かつ、利用者のプライバシも保証するところに特徴がある。

【００３５】図４は、ラベルの判定をネットワーク上の独立したコンテンツ監視装置で行う１実施例の構成を示したブロック図である。

【００３６】図４で、４１３と４６３は暗号化通信手段、４６２は判定手段、４６０は、ラベルと操作画面の記録の有無の規則をしるした規則表である。この例では、各計算機でいったんラベルを復号し、別の暗号化プログラム４１３を用いて暗号化し、ラベル判定用にコンテンツ監視装置４５１に送る。４６０の規則表をもとに操作履歴の記録の必要性を判定した結果を返すのが特徴である。

【００３７】図５以降は、本発明に関連する装置や手順を示した説明図である。

【００３８】図５は、各計算機でのラベルを検出する手順を示した流れ図である。

【００３９】図６は、計算機とファイアウォールでのラベルを生成、分離するプログラムの配置を示したブロック図である。この例では、ラベルと通信データとを結合し、暗号化してある（カプセル化）データを、解決するのが特徴である。

【００４０】図７は、ファイアウォールで暗号化した通信データを、各計算機で復号する手順を示した流れ図である。この例は、暗号鍵と復号鍵が異なる非対称暗号方式を用いた実施例である。

【００４１】図７で、７０４は、ファイアウォールにおいて、あらかじめ利用者別あるいは計算機別に登録されている公開鍵が存在しないので、ファイアウォール用に登録してある公開鍵を利用するステップ、７１４は、各計算機において、復号できない場合に、改めて、自ら復号可能な公開鍵を添付し、ファイアウォールに再送し、再暗号化を依頼するステップである。

【００４２】図８は、各計算機で暗号化した通信データを、ファイアウォールにおいて、復号可能であるかを検査する手順を示した流れ図である。８０４は、機密の低いネットワークの通信先の公開鍵がないので、ファイアウォール用に登録してある公開鍵を利用するステップ、８１４は、各計算機において、復号できない場合に、依頼するステップである。

【００４３】図９は、各計算機の構成で、とくに通信データを暗号化を行うための鍵管理に可搬型カードを用いる場合の構成を示したブロック図である。カード９２１は、ファイアウォールの公開鍵９２１と利用者の暗号鍵９２２を内蔵している。この例は対称暗号アルゴリズムと非対称暗号アルゴリズムとをミックスさせたセッション鍵の交換方式の一実施例を示している。９１４はカード９２１を読み取る装置である。

【００４４】また、９１３はディジタルカメラである。ＣＲＴ９１２の操作画面９３０だけでなく、操作者の顔写真を同時に記録するのが目的である。

【００４５】以上の図面を使って、本実施例の詳細な説明をしていく。

【００４６】ラベルを検出する手順について、図１、図２ならび図５を用いて説明する。

【００４７】図２はこのラベルを利用するシステムの全体構成を説明する図である。

【００４８】計算機２０１は機密レベルの低いネットワーク２０２（たとえばWAN）、計算機２０３は２０２に比べて機密レベルの高いネットワーク２０４（社内ＬＡＮ）に接続する。２０２と２０４との間にファイアウォール２１０が存在する。ファイアウォール２１０には一時記憶装置２１１（たとえば、磁気ディスク、フラッシュメモリ）が接続し、下記に示すようなプログラムやデータ、鍵等を格納する。

【００４９】計算機２０１から計算機２０３に対し、通信データ２２０を送受信する際に、ラベル２４１をファイアウォール２１０で添付あるいは削除する様子を示す。

【００５０】ファイアウォール２１０は、各通信データの機密性に応じて通信データの配送、通過停止等の処理を行う。具体的には、２０４内を流れる通信データには、機密性を示すラベルを添付し、計算機２０３では、このラベルを利用した、アクセス制御を行う。ファイアウォール２１０には、２０２から２０４へ流れる通信データにラベルを添付する手段２３１、ならびに２０４から２０２へ流れる通信データ２２０から削除する手段２４１が常駐する。

【００５１】とくに、ラベル２４１を、計算機２０３やネットワーク２０４上で改ざん、盗聴を防ぐ、ラベル暗号化機能も設けることが望ましい。暗号手段２４３は添付手段２３１と、復号手段２４２は破棄手段２４２と連

動する。本実施例では、説明を簡単にするために、非対称暗号を用いた実施例を、以下で説明していく。

【００５２】計算機２０３の暗号手段２４３とファイアウォールの復号手段２４２、計算機２０３の復号手段２３３とファイアウォールの暗号手段２４２とはそれぞれ対応する暗号・復号プログラムである。２３０、２４０、２４４、２３４は、暗号・復号で使用する鍵である。ファイアウォール２１０の公開鍵２３０で暗号化したラベルを計算機２０３の秘密鍵２３４で復号する。計算機２０３の公開鍵２４４で暗号化したラベルをファイアウォール２１０の秘密鍵２４０で復号する。

【００５３】本実施例では、とくに、情報データ２２０の送信先・受信元のアドレス（たとえばＩＰアドレス、ＭＡＣアドレス）、サービスの種類（たとえばポート番号：ニュース、ＦＴＰ、ＨＴＴＰ等）、送信先・受信元の利用者ＩＤ等の属性情報とラベル２２１との関連を規定した対応表２２２をファイアウォール２１０に備えることが望ましい。対応ラベルを複数用意し、きめ細かい制御を行うことが可能となる。

【００５４】図２のシステム構成を踏まえ、図１を用いて、計算機２０３でのコンテンツ監査方法の流れを説明する。

【００５５】ファイアウォール２１０からラベル２３１を添付した通信データ２３０をダウンロードし（１１０）、暗号化している場合には復号操作も含め、一定形式でのラベルを抽出する（１１１）。もし抽出できない場合には（１１２）、１４０以下のエラー処理を行う。ラベルの内容、たとえば機密を示す種別、利用できる範囲を読み取り、たとえば暗号化ともに行われたディジタル署名をもとに、ラベルが偽造されるかどうかを判定する（１１４）。さらに、ラベルをもとに機密レベル判定する（１１６）。とくにローカルマシンでは判定できない場合には、ネットワーク上のラベル監視サーバ（後述４６２）に問い合わせる、記述されているラベルと機密レベルとの関係（セキュリティ基準にあわせ、指定されている）を検索する（１１５、１３０、１３１）。

【００５６】機密レベルが判定でき、履歴収集が必要なレベル（たとえば代表的なセキュリティ基準ＴＣＳＥＣでは、Ｂ１レベル以上）のデータと判定された場合に、監視を開始する（１１７）。たとえば、キーボードやマウス等の入力により、ダウンロードした通信データに対するインタラクティブな画面操作が行われる。外部システムへの送信（たとえば電子メール、ＦＴＰ）、ローカルな可搬媒体（たとえば磁気ディスク、ハードディスク）への複写に関する操作を行うことで、ＯＳで規定しているシステム関数、たとえばWindowsでいえばWinsockやFile I/Oが呼ばれることを検出する（１２１）、あるいは一定時間ごとに、たとえば１分おきに（１２５）、操作画面のイメージ、Bitmapをファイルに記録する（１２２）。なお、操作者を写すディジタルカメラが、２０３に接続されているのならば、画面操作同時に記録することで、一層効果的な履歴を残すことができる。ダウンロードした通信データに関する操作するプログラムを終了する（１２４）しない場合には、再びステップ１２１へ戻る（１２３）。

【００５７】ラベルを用いた機密レベルの判定に関するエラー処理（１４０、１４１）について述べる。ラベルを抽出できない、ラベルが偽造である場合には、不正コンテンツであると端末の利用者に警告を表示し、終了か継続するかどうかの判定を求める（１４０）。利用者が「終了」を選択した場合は、ダウンロードした通信データに関するアクセスを終了する（１４１）。「継続」を選択した場合は、操作履歴を採ることに利用者が同意したと見なし、ステップ１２０へ進む。

【００５８】図１におけるラベル抽出処理１１１を詳細に述べる。とくに、コンテンツ流通に関し、暗号を用いたカプセル化の一実施例を図５および図６を用いて、説明する。

【００５９】抽出処理に対応し、ファイアウォール２１０でのラベル添付処理を説明する。

【００６０】図６において、通信データ２３０は、６１０のコンテンツの本体であるデータ部とコンテンツの属性（シリアル番号、サービスの内容など）を示すヘッダ部６１１とに分かれる。このような属性のヘッダ部に対応し、添付するラベル６１２を決定する（本実施例では"Project"というキーワードに対し、"SECRET,R&D"と
いうラベルが対応）ための対応表２２２に照らしあわるのが、添付手段２３１である。６１２を６１１および６１０と結合し、公開鍵２３０を用いて暗号化する。

【００６１】このように暗号化した通信データとラベルを分離するのが、抽出処理１１１である。基本的には、添付処理に対応して、逆の処理を行う。秘密鍵２３４を用いて、平文に復号する。図５で、暗号化された通信データかを判定する（５０１）。判定方法としては、たとえばRFC1847(Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted)で示しているような属性と属性値とを組みとしたタグで判定する方法でおこなう。判定できた場合には、秘密鍵２３４を用いて復号処理を試み（５０３）、復号し（５０４）たのちに、ラベル部分を含んだヘッダ部分（６１２）の範囲を判定し（５０５）、切り取った後（５０６）に、定められたラベルの形式にあわせ（５０７）、各項目（たとえば、機密レベル、カテゴリ）等の検査（５０８）を行う。

【００６２】次に、図３を用いて、計算機２０３のステップ１２２で一次記憶装置３０１に記録した履歴３２３を、暗号化し、収集するシステムの構成を説明する。

【００６３】３５１は、監査人専用の計算機であり、３５２はＣＲＴ、３５３は履歴を蓄積する一次記憶装置である。

【００６４】計算機２０３には、履歴を一次記憶装置３

０１に記憶するプログラム３１０、３０１に記憶した履歴３２３を暗号化するプログラム３１１、暗号化した履歴を送付するプログラム３１２を備える。

【００６５】計算機３５１には、鍵生成ならびに計算機２０３に鍵配布するプログラム３６１、履歴をハードディスク３５３に収集するサーバプログラム３６２、収集した履歴３２４を復号し、ＣＲＴ３５２に表示するプログラム３６３を備える。３２１と３２２は、プログラム３６１が生成する暗号鍵である。３２１は履歴３２３を暗号化する公開鍵、３２２は履歴３２４を復号するための秘密鍵である。あらかじめ、あるいは暗号プログラム３１１が用いる場合に備えて、鍵３２１は計算機２０３に送られ、一次記憶装置３０１に記憶する。

【００６６】本実施例では、監査者用の公開鍵を使って、暗号化した後に、適宜管理者用の専用装置に送り、履歴の改ざん、盗聴、各計算機でのディスクの消費を防ぐところにある。

【００６７】次に、図４を用いて、計算機２０３のステップ１３０で、コンテンツに添付されたラベルを抽出し、サーバ４５１に問い合わせるシステム構成を説明する。

【００６８】４５１は、管理者専用の計算機であり、４５２はＣＲＴ、４５３はラベルと機密レベルとの対応表４６０を格納する一次記憶装置である。

【００６９】計算機２０３には、一次記憶装置４０１に記憶したコンテンツ４２０ならびにラベル４２３を復号するプログラム２３３、コンテンツをラベルを検査するプログラム４１２、ラベルに関する問い合わせを行う、とくにラベルに関する情報をそのまま暗号化してプログラム４１３を備える。

【００７０】計算機４５１には、鍵生成ならびに計算機２０３に鍵配布するプログラム４６４、プログラム４１３からの問い合わせに応じ対応する暗号通信プログラム４６３、４６３から呼び出され、暗号化したラベルと機密レベルとの対応表４６０とを比較し、操作履歴を記録すべきかどうかを判定するプログラム４６２、プログラム４６２からさらに呼び出され、ＣＲＴ４５２に、機密アクセス違反が発生し、操作履歴を記録するメッセージを表示する警告プログラムを備える。また、対応表４６０の内容を管理者が設定するなプログラム４６１も備える。４２１と４２２は、プログラム４６４が生成する暗号鍵である。４２１はラベル４２４を暗号化する公開鍵、４２２はラベル４２４を復号するための秘密鍵である。あらかじめ、あるいは暗号プログラム４１３が用いる場合に備えて、鍵４２１は計算機２０３に送られ、一次記憶装置４０１に記憶する。

【００７１】本実施例では、ラベルに対応する機密性の意味付けをネットワーク上の管理者が定めた対応表４６０上の規則に応じて、動的に変更できるところにある。

【００７２】図７および図８を用いて、ファイアウォール２１０と計算機２０３での暗号通信の手順を示す。

【００７３】図７は、ファイアウォール２１０での暗号プログラム２３２、計算機２０３での復号プログラム２３３の処理を示す。ファイアウォール２１０に対応表２２２を備え、行き先の計算機や利用者にあわせて異なる暗号鍵を利用するところに特徴がある。ここでは、ネットワークのパケットのレベルで暗号化を行う例を示す（アプリケーション層での暗号化でも、ＩＰアドレスやポート番号の変わりに、利用者ＩＤ等の情報を使って同様にして行うことができる）。

【００７４】まず、コンテンツが流れてきたネットワークの機密レベルを送信元のＩＰアドレスで判定し（７０１）、暗号化が必要な場合は、さらに受信先の計算機２０３のＩＰアドレスをパケットから抽出し（７０２）、受信先のＩＰアドレスに対応した公開鍵２３０を使って暗号化し（７０５）、もし公開鍵２３０がないときには（７０３）、ファイアウォール２１０の公開鍵を使って暗号化する（７０４）。暗号化したパケットを計算機２０３へ送付する（７０５）。計算機２０３では、流れてきたパケットが復号が必要な場合には、公開鍵２３０に対応する秘密鍵２３４を用いて復号する（７１２）。復号できない場合には、ステップ７０４の処理が行われたと判定し（７１３）、ファイアウォールに自分の公開鍵２３０とパケットを送り、ファイアウォール内で、いったんパケットを復号したのちに、公開鍵２３０で再暗号化する（７１４）。

【００７５】本実施例では、ファイアウォールに、外部の計算機との通信を頻繁に行わない計算機では、再暗号化処理を設けることで、応答性能とセキュリティを満足できるようにしてあるところに特徴がある。

【００７６】図７と逆に、機密の高いネットワークから低いネットワークへのパケットの流れを制御する、ファイアウォール２１０での復号プログラム２４２、計算機２０３での暗号プログラム２４３の処理を図８を使って示す。

【００７７】ファイアウォール２１０に対応表２２２を備え、行き先の計算機や利用者にあわせて異なる復号鍵を利用するところに特徴がある。ここでは、図７同様にネットワークのパケットのレベルで復号化を行う例を示す。

【００７８】計算機２０３において、他の計算機へデータを送る場合暗号が必要であると判定し（８０１）、各計算機のＩＰアドレスにあわせた公開鍵で暗号化する（８０５）。送信先がとくに機密レベルが低いネットワーク２０２に属する計算機２０１であると判定した場合は（８０３）、ファイアウォール２１０の公開鍵２３０で暗号化する（８０４）。暗号化した通信データをパケットとして送信する（８０６）。

【００７９】ファイアウォール２１０において、送信元の計算機２０３のＩＰアドレスをパケットから抽出し、

通信データが流れてきたネットワークの機密レベルを送信元のＩＰアドレスで判定し（８１１）、ファイアウォールの秘密鍵２４０を使って復号する（８１２）。復号できた場合には、ファイアウォールから機密レベルの低いネットワーク２０２の計算機２０１へ送付（８１５）、復号できない場合には、ファイアウォールの通過を許さない（８１４）。

【００８０】本実施例では、外部の計算機にデータ通信を行う場合は、必ずファイアウォールでファイアウォールで平文に復号し、外部への機密持ち出しを監視できるようにしてあるところに特徴がある。

【００８１】以上、計算機のＩＰアドレスを利用して、暗号鍵を設定する実施例で述べた。以下では、アプリケーション層の利用者ＩＤを利用して、暗号鍵を設定する別の実施例を述べる。

【００８２】図９は、可搬型媒体（たとえばＰＣＭＣＩＡカード９２０）を用いて、利用者ＩＤに対応した暗号鍵を管理するシステム構成を説明したブロック図である。計算機２０３は、ハードディスクやメモリ、ＣＰＵを内蔵した本体９１１、ＣＲＴ９１２、ディジタルカメラ９１３、カードリーダ９１４、キーボード（マウス）９１５で構成する。ディジタルカメラ９１３、カードリーダ９１４は本体９１１の付属装置である。

【００８３】ＣＲＴ９１２には操作画面９３０（マルチウィンドウ）が映し出される。キーボード９１５を用いて操作する操作画面９３０ならびに、ディジタルカメラ９１３で写された利用者の顔写真を履歴として記憶する。

【００８４】カード９２０には、利用者の秘密鍵９２３ならび公開鍵９２４と、ファイアウォールの秘密鍵２４０に対応する公開鍵９２５とを内蔵し、備えているところが特徴である。ファイアウォールには、公開鍵９２４のコピーである公開鍵２３０と、ファイアウォールの秘密鍵２４０とを備えている。可搬媒体９２０を用いて、カードリーダ９１４を備え、プログラム２３３やプログラム２４３を常駐する不特定の計算機で利用することで、利便性が増す。

【００８５】

【発明の効果】本発明により従来の問題点が解決される。

【００８６】(1) 契約外のコンテンツの流通を許さない。

【００８７】各計算機で、ラベルを参照し、正規のラベルが添付していないコンテンツの複製や他システムへの転送が不正であることを明確にするので、不正流通の影響を局所化できる。

【００８８】(2) 操作画面を履歴として記録することを示し、利用者の無断複製を抑制できる。

【００８９】利用者に計算機上でコンテンツの複製する操作が履歴として残ること、あわせて無断複製が発覚した際の罰則を示すことで、違反行為を抑制できる。

【００９０】また、操作画面や顔写真をビジュアルな履歴として記録することで、組織外の監査者が、業務の内容に関わらず客観的に不正行為の有無を判定できる別の効果もある。

【００９１】本発明では、組織外の第３者である監査者が作業する専用の監査装置をネットワーク上に設け、各計算機での操作履歴を転送し、蓄積する。

【００９２】この際に、各計算機では監査者の公開暗号鍵を用いて、操作履歴を暗号化する。監査者は、監査要求があった際に初めて、別途厳重に管理した秘密暗号鍵を用いて、蓄積された操作履歴を復号する。このように、各計算機で操作履歴を暗号化し、監査装置に転送することで、監査者以外の利用者や管理者が、操作履歴を参照し、改ざん、隠滅することを防止する。

【００９３】本発明では、組織内の管理者が作業する専用の監視装置をネットワーク上に設け、ラベルに対応し、操作履歴を記録する必要性を監査規則表をもとに判定する。

【００９４】このため、管理者が、組織（ドメイン）内の規範に従い、各計算機でのコンテンツのアクセスや複製の制御や管理ができ、また規範の変更にともなうメンテナンス作業は、監査規則表の書き換えだけですむ。また、監査規則表の設定により、すべてのコンテンツのアクセスや複製について操作履歴をとる必要がなく、操作履歴を蓄積する記憶媒体（ハードディスク）の浪費の防止ならび利用者のプライバシーの保護に対応できるシステム運用が実現できる別の効果もある。

【００９５】本発明では、専用のファイアウォールをネットワーク上に設け、通信データの入出力に対応し、ラベルの生成や破棄処理をおこなう。機密レベルが高いネットワーク（たとえばＴＣＳＥＣのＢレベル以上）に属する計算機に、通信データのラベルを読み取る機能（ミドルソフトウエアあるいはＯＳ）を設けている。

【００９６】このため、管理者が、組織（ドメイン）内の規範に従い、ファイアウォールを境に機密レベルが異なるドメイン間でのコンテンツのアクセスや複製の制御ができる。

【００９７】さらに、専用のファイアウォールでは、コンテンツの参照者を限定した暗号化鍵でラベルを暗号化する。しかも、コンテンツを復号できる復号鍵は、通信のたびに内容を変更するセッション鍵を利用者別に配布された可搬型カード（たとえばSmart Card, PCMCIAカード）に格納する。復号したコンテンツは、利用を終えた段階で破棄する。

【００９８】このため、可搬型カードを用いて、コンテンツのファイアウォールから各計算機へのダウンロード（１次コピー）できるが、他システムへの転送やハードディスクへの別名でのファイル格納（２次コピー）を抑制できる。

【図面の簡単な説明】

【図１】計算機におけるコンテンツ監査方法のフローチャート。

【図２】機密レベルが異なるドメインを接続する本発明のファイアウォールのブロック図。

【図３】端末の操作画面の履歴を蓄積する本発明の監査装置のブロック図。

【図４】端末の操作画面の記録の必要性を判定する本発明の監視装置のブロック図。

【図５】各計算機でのラベルを検出する手順を示したフローチャート。

【図６】ラベルを生成し、分離するプログラムの配置を示したブロック図。

【図７】ファイアウォールで暗号化した通信データを、各計算機で復号する手順を示したフローチャート。

【図８】計算機でおいて暗号化した通信データを、ファイアウォールにおいて、復号可能であるかを検査する手順を示したフローチャート。

【図９】本実施例の計算機端末の構成を示したブロック図。

【符号の説明】

２０１、２０３…計算機、

２１０…ファイアウォール、

２３２、２３１、２４１、２４２…ファイアウォールに常駐するプログラム、

３１０…履歴記録プログラム、

４５１…管理者用端末、

３５１…監査者用端末、

９１３…カメラ、

９２０…カード。

【図２】

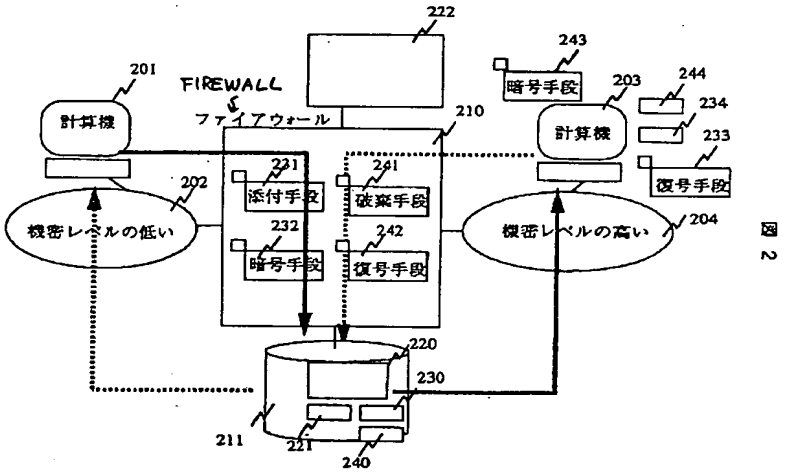
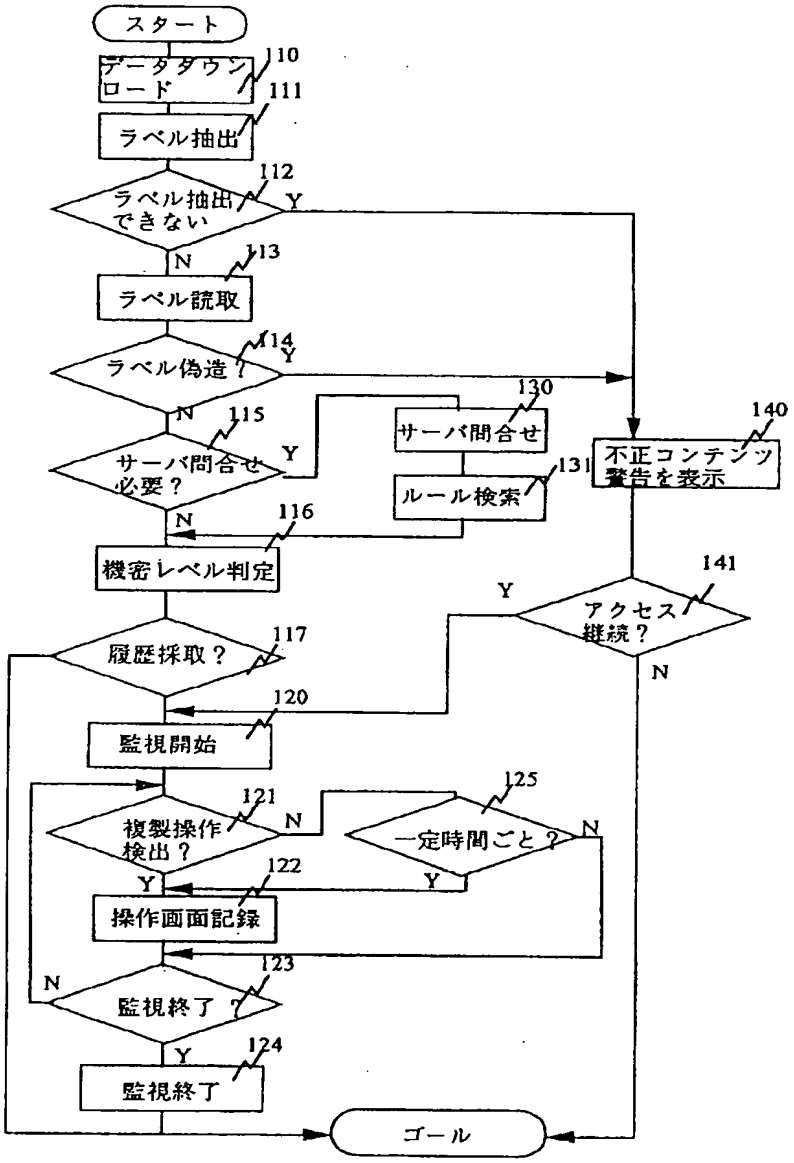


図２

【図１】

図　１


スタート
データダウンロード
10
ラベル抽出
111
ラベル抽出できない
112
Y
N
ラベル読取
113
ラベル偽造？
114
Y
N
サーバ問合せ必要？
115
Y
N
サーバ問合せ
130
ルール検索
131
不正コンテンツ警告を表示
140
機密レベル判定
116
アクセス継続？
141
Y
N
履歴採取？
117
監視開始
120
複製操作検出？
121
N
Y
一定時間ごと？
125
N
Y
操作画面記録
122
監視終了？
123
N
Y
監視終了
124
ゴール

【図３】

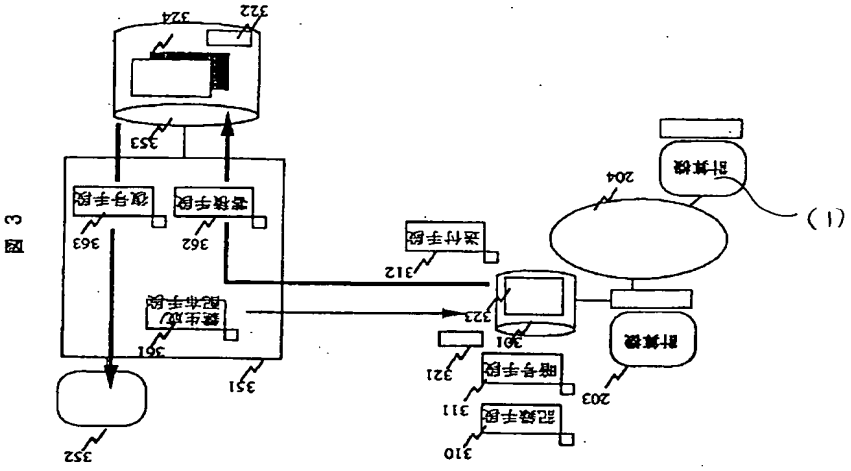


図３

【図４】

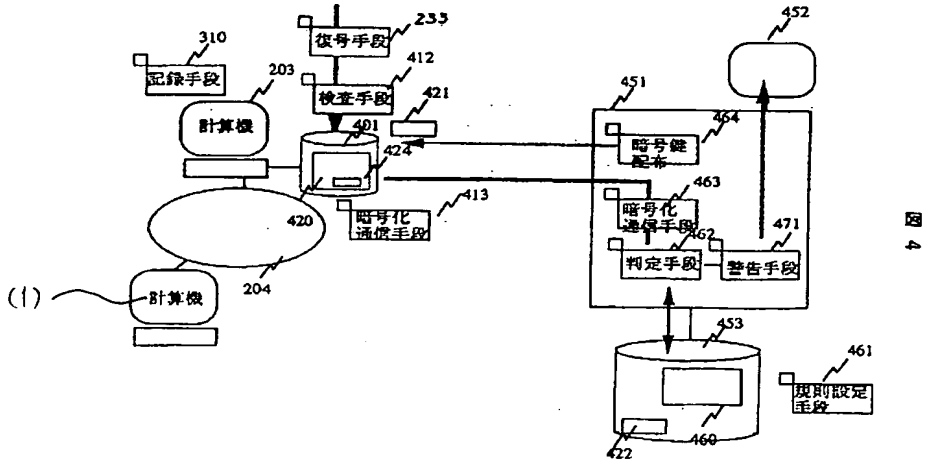
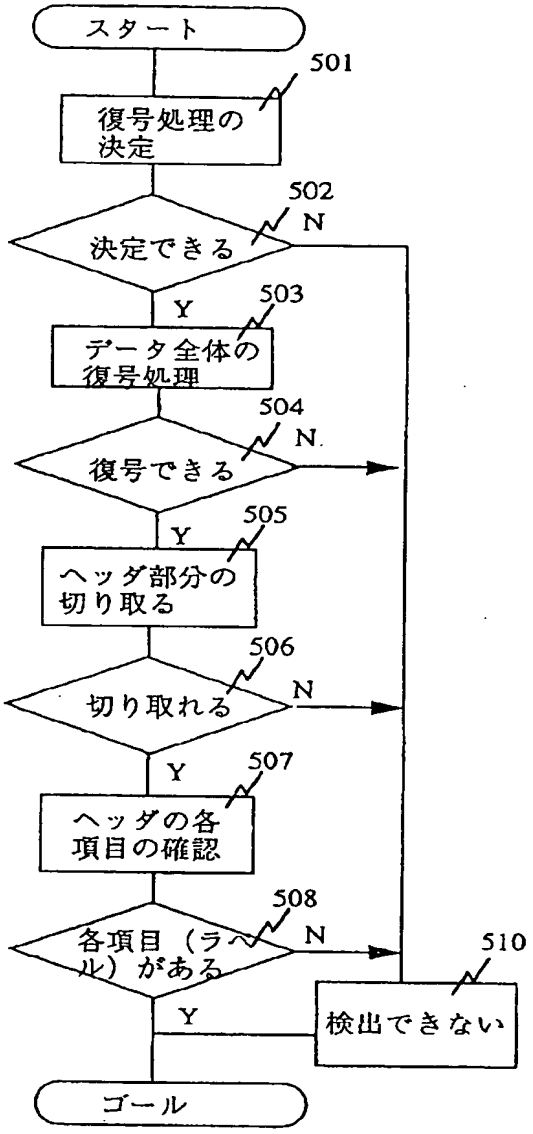


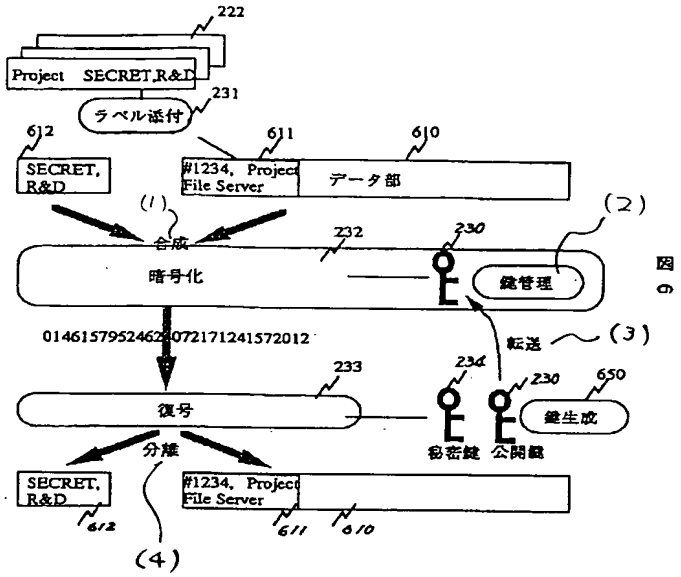
図４

【図５】

図　５

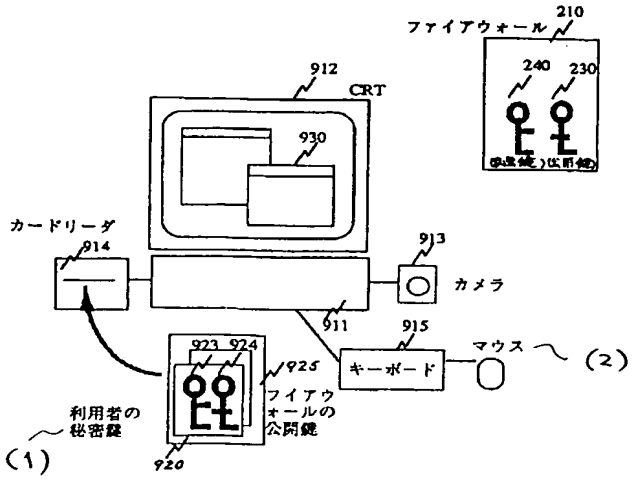


【図６】



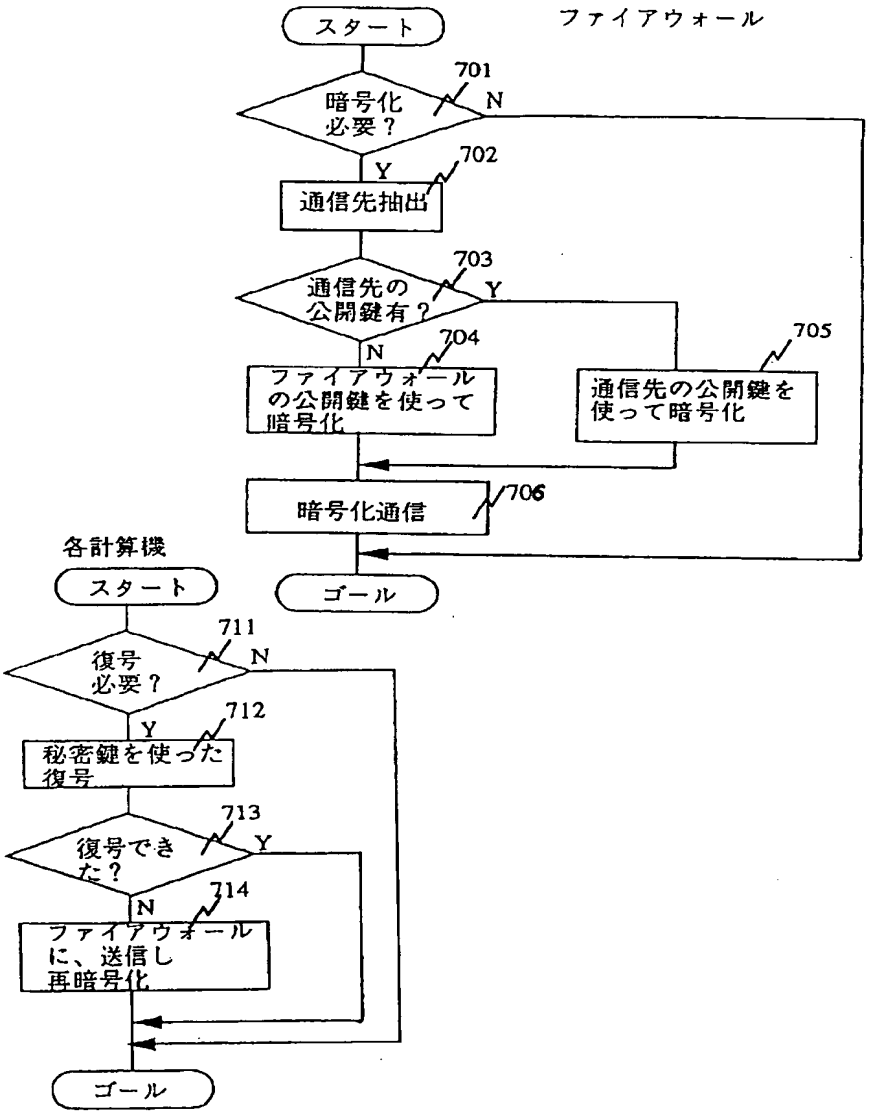
【図９】

図　９



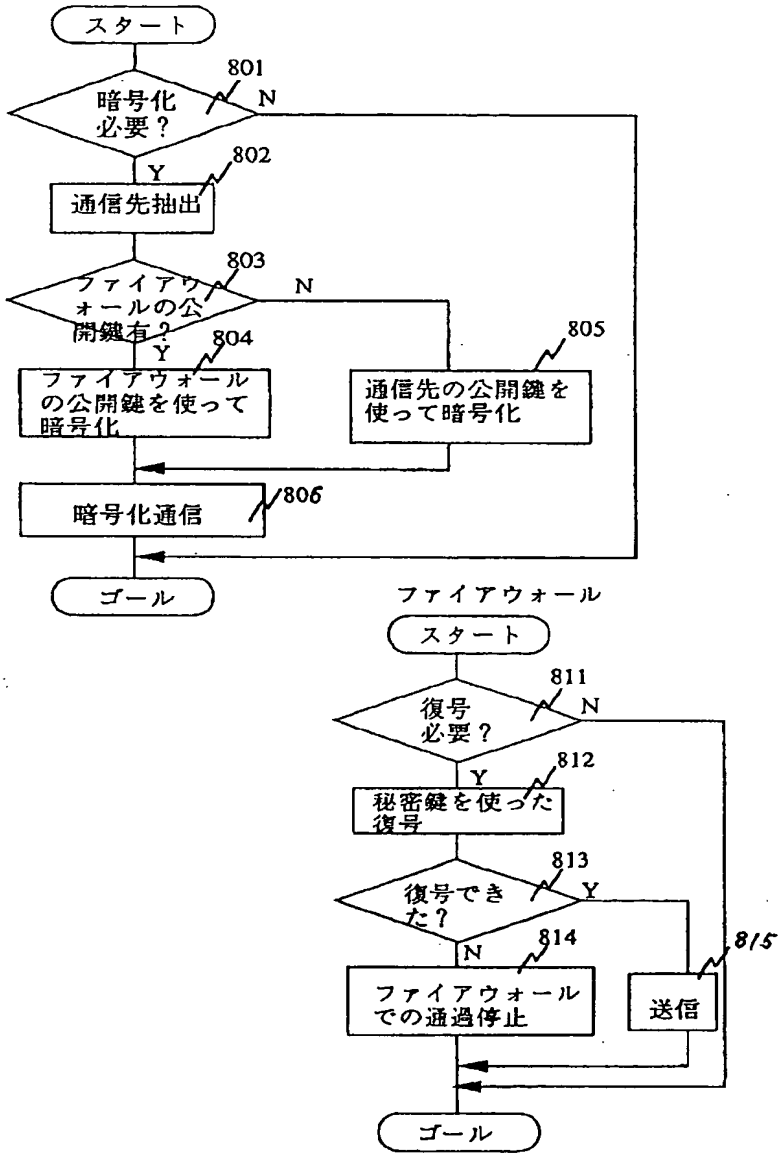
【図７】

図　７



【図８】

図 8



フロントページの続き

(72)発明者　難波　電
神奈川県川崎市麻生区王禅寺1099番地株式会社日立製作所システム開発研究所内

Translation of JP-A-10-111855

Laid-Open (KOKAI) Date: April 28, 1998
Application No. Hei 08-264051
Application Date: October 4, 1996

[Title of the Invention]
METHOD AND APPARATUS FOR MONITORING COMMUNICATION DATA

[Abstract]
[Problem] A system administrator of an intranet has the following problems in circulating content in the intranet.
(1) Restriction of circulating contents out of contract without permission;
(2) Restriction of copying of contents without permission.
[Solving Means] (1) Controlling circulation of contents within a network by providing a label unique to a business enterprise.
(2) Recording an operation screen image in copying content and mug-shot of a user as history.
(3) Especially, method and administration mode for recording the history of (2) are determined depending upon the kind of the label of (1).

[Scope of Claim for a Patent]
[Claim 1] A communication data monitoring method for a plurality of computers connected to a network, comprising the steps of transferring communication data and a label relating to said communication data between said computers, and making reference to said label and making judgment of security level of said communication data, wherein said method further comprises a step of detecting an effective security level within a range of said computers or said network on the basis of said label, a step of accessing or copying the communication data, and a step of recording a mug-short of an operator or an operation screen image of each computer as history.
[Claim 2] A firewall for temporarily storing communication

data flowing between networks setting mutually different security levels, which is used by a computer connected to the network having a higher security level as a communication data accumulation apparatus, comprising means for adding a label indicative of an attribute of a security level to the communication data received from a network having a lower security level, and means for deleting said label from the communication data to be transmitted to the network having lower security level.

[Claim 3] A communication data monitoring apparatus connected to a plurality of computers via a network, and presenting operation history of access and copied communication data in said computers to an auditor, comprising key generating means for generating a public key of the auditor and transmitting to said computer, history accumulating means for accumulating encrypted operation history of mug-shot of the operator and screen image content, and history decrypting means for decrypting the operation history by a secret key of the auditor.

[Claim 4] A communication data monitoring apparatus connected to a plurality of computers via a network, and presenting operation history of access and copied communication data in said computers to an auditor, comprising rule setting means for recording a security level attached to the communication data and a correspondence table of monitoring rule, and security judgment means for retrieving said correspondence table in response to an inquiry of each computer and returning necessity/un-necessity of obtaining of history relating to said communication data.

[Claim 5] A communication data monitoring method as set forth in claim 1, further comprising a step of displaying an advisory message indicating access prohibit of communication data on an operation screen of the computer upon non-detection

of the label indicative of a security level.

[Claim 6] A communication data monitoring method as set forth in claim 1, further comprising a step of decrypting the label and communication data by an independent encryption key of each user or each computer.

[Claim 7] A firewall as set forth in claim 2, further comprising means for accumulating the communication data transmitted from a computer of the network having a lower security level, and including label attaching means holding an encryption key enabling at least one computer and at least one user of a network having a higher security level to decrypt, for encrypting data combined by communication data and the label by using said encryption key to encrypt the label.

[Claim 8] A firewall as set forth in claim 2, further comprising means for accumulating encrypted data transmitted from a computer of the network having a higher security level, including label attaching means holding a decryption key for decrypting the encrypted data, for decrypting cipher data in which the communication data and the label are contained by using said decryption key to separate said communication data and said label, and means for accumulating history of sending said communication data to a network having a lower security level according to a security label.

[Claim 9] A portable card to be connected to a computer for receiving communication data and a label where a plurality of computers and a firewall are connected via a network, and for use in decrypting encrypted communication data and a label, wherein encrypting keys generated in session with firewall independently per user and security label are accumulated.

[Detailed Description of the Invention]

[0001]

[Technical Field Pertinent to the Invention] The present invention relates to a technology for certainly maintaining

security of communication data in a computer network.

[0002]

[Prior Art] According to spreading of the Internet and intranet, the following problems are caused upon communicating program (hereinafter referred to contents), such as so-called multimedia data, software and so forth through a network.

[0003] (1) Copies of contents by unspecified number of users: By computers (personal computers) at a terminal end of flow, content can be easily copied. Furthermore, since an owner cannot monitor the condition of end PCs, it is difficult to claim for intellectual property right.

[0004] (2) Charge incurred upon using content:
Pay-later system in which a user may pay the charge only after use of the content, not at a stage at which the owner having the right for charging sends out the content. However, similarly to the problem (1), since the owner cannot monitor the condition of the end PCs, it is difficult to charge the account to the user.

[0005] As an approach for these problems, a system and apparatus of super-distribution are designed so that an owner circulates content attaching own information as an electronic label and a user pays for the charge to the owner indicated on the label depending upon a use amount of the content. Super-distribution has been disclosed in Ryoichi MORI, Seiji KAWAHARA and Yasuhiro OTAKI "Super-distribution: Electronic Technology for Processing of Intellectual Property Right", Information Processing Society of Japan, Vol. 37, No. 2, February 1996.

[0006]

[Problem to be Solved by the Invention] However, in the known art, there are following unsatisfactory points for the provider (enterprise) of an intranet and a system administrator.

[0007] (1) Circulation of contents without permission can not

be restricted.

The system administrator provides a server device accumulating contents by installing the contents using a portable medium, such as CD-ROM, DVD or downloading using a communication program, such as FTP, WWW or the like. A general user uses the content by accessing to the server device.

[0008] However, it is possible that the general user loads the content without permission of the owner to circulate in a network.

[0009] At this time, by loading the contents out of designing, a resource of the computer, such as a hard disk, a network and so forth can be wasted to hinder businesses. Otherwise, invasion of virus in the network may cause economical damage of data destruction.

[0010] The system administrator is required to prove to a provider that a user does not circulate contents without permission.

[0011] (2) Activity of copying contents without permission can not be restricted.

Between an owner and an enterprise, a site licensing contract is established for permitting copying contents only for use in the computers connected to the internal network of the enterprise. The owner may certainly receive a charge for the contents from the enterprise. The enterprise may eliminate use charge and load for administration of the contents by establishing a bulk contract.

[0012] However, it is possible that a general user copies the contents without permission of the system administrator or the owner and uses them in the network or computer out of contract. In such a case, when abusing comes into the light, the owner may sue the enterprise for violation of contract.

[0013] The system administrator is required to prove to the owner that a user has not copied contents without permission.

[0014]

[Means for Solving the Problem] In order to accomplish the above-mentioned objects, an effective security level within a range of said computers or said network is detected on the basis of the label, and upon accessing or copying communication data, a mug-short of an operator or operation screen image of each computer is recorded as history.

[0015] Particularly, when the security level is detected, (1) an advisory message indicating access prohibit of communication data is displayed on the operation screen of a computer upon non-detection of the label indicative of security level.

[0016] (2) A label encrypted by the firewall or the like is decrypted by an independent decryption key per user or computer.

[0017] The foregoing is desirable.

[0018] A monitoring apparatus is provided on the network.

[0019] The monitoring apparatus is preferably an apparatus comprising key generating means for generating a public key of an auditor and transmitting to said computer, history accumulating means for accumulating history encrypted for each computer by using the public key of the auditor, and history decrypting means for decrypting operation history by a private key of the auditor.

[0020] The monitoring apparatus is provided on the network.

[0021] The monitoring apparatus is desirably an apparatus comprising rule setting means for recording a correspondence table between a label indicating security attached to the communication data and a monitoring rule, and security judgment means for retrieving said correspondence table in response to an inquiry of a computer and returning necessity/un-necessity of obtaining of history relating to said communication data.

[0022] On the other hand, a firewall provided on the network

premised to the foregoing label control has means for attaching a label indicative of attribute of a security level to communication data received from a network having a lower security level, and means for deleting said label from the communication data to be transmitted to a network having a lower security level.

[0023] Particularly,

(1) There is held an encryption key enabling at least one computer and at least one user of a network having a higher security level to decrypt, and data combined by communication data and a label is encrypted by using said encryption key to encrypt the label.

[0024] (2) There is possessed a decryption key for decrypting encrypted data in which communication data and a label are contained by using said decryption key, said communication data and said label are separated for deleting the label, and history for sending said communication data to a network having a lower security level is accumulated depending upon a security label.

[0025] The foregoing is desirable.

[0026] On the other hand, a portable card for label-decrypting is used in each computer.

[0027] In the portable card, it is desirable that encrypting keys are accumulated independently per user and security label to be used upon decrypting the label and the communication data encrypted by a firewall.

[0028]

[Mode for carrying Out the Invention] Embodiments of the present invention will be discussed in detail with reference to the drawings.

[0029] Fig. 1 is a flow diagram of a content monitoring method in a computer to which the present invention is applied.

[0030] In Fig. 1, 111 denotes a process for extracting a label from a content, 116 denotes a process for making judgment of

a security level of the content on the basis of the extracted label, 121 denotes a process for detecting copying operation of the content by a user, 122 denotes a process for recording an operation screen image. It is characterized by making judgment whether history (operation screen image or mug-stop of the user) is to be recorded or not depending upon a security level.

[0031] Fig. 2 is a block diagram showing one embodiment of a firewall attaching the label of the present invention.

[0032] In Fig. 2, 231 denotes a program for attaching the label, 232 denotes a program for encrypting communication data together with the label, 241 denotes a program for revoking the label, and 242 denotes a program for decrypting the label. The firewall 210 is connected to networks having different security levels, and is characterized by encrypting communication data transmitted from a network having a lower level, and decrypting communication data transmitted from a network having a higher level.

[0033] Fig. 3 is a block diagram showing a construction for encrypting operation history recording by the present invention, transmitting it to a server for an auditor and accumulating it. This embodiment is one using an asynchronous encryption method in which an encryption key and a decryption key are different.

[0034] In Fig. 3, 361 denotes a key (generation) distribution program for (generating a public key 321 and a private key 322 of an auditor) and distributing the public key 321 to each computer recording the history. Numeral 362 denotes a program for accumulating operation history 324 of each computer, 363 denotes a program for decrypting the operation history 324 and presenting to the auditor. In Fig. 3, it is characterized by keeping secret of business by encryption at each computer and send it to an auditor sever, and giving guarantee for privacy

of the user.

[0035] Fig. 4 is a block diagram showing a construction of one embodiment in which label judgment is implemented by an independent content monitoring apparatus on a network.

[0036] In Fig. 4, 413 and 463 are encryption communication means, 462 denotes judgment means, 460 denotes a rule table indicating presence/absence of rules recording of labels and operation screen images. In this example, a label is once decrypted by each computer, encrypted using another encrypting program 413, and sent to a content monitoring apparatus 451 for label judgment. It is characterized by returning the result of judgment for necessity of recording of operation history on the basis of the rule table.

[0037] Fig. 5 and subsequent drawings are explanatory illustration showing an apparatus and a procedure relating to the present invention.

[0038] Fig. 5 is a flow diagram showing a procedure for detecting the label in each computer.

[0039] Fig. 6 is a block diagram showing an arrangement of programs for generation and separation of the label in the computer and the firewall. This embodiment is characterized by solving data combined by the label and the communication data and encrypted (encapsulated).

[0040] Fig. 7 is a flow diagram showing a procedure for decrypting communication data encrypted in a firewall by each computer. The shown embodiment is one employing an asynchronous encryption method in which an encryption key and a decryption key are different.

[0041] In Fig. 7, 704 denotes a step of using a public key registered in a firewall for absence of a public key preliminarily registered for each user or each computer, 714 denotes a step of attaching a self-decryptable public key, re-transmitting it to the firewall, and requesting re-

encryption, when decrypting is not possible in each computer.

[0042] Fig. 8 is a flow diagram showing a procedure for inspection of communication data encrypted by each computer as to whether decrypting is possible or not in the firewall. 804 denotes a step of using the public key registered for the firewall since there is no public key at a communication destination of a network having a lower security, and 814 denotes a step of sending a request when decrypting is not possible in each computer.

[0043] Fig. 9 is a block diagram showing a construction of each computer, especially, a construction in a case where a portable card is used for key management for encrypting communication data. A card 921 incorporates the public key 921 of the firewall and an encryption key 922 of a user. The example shows one embodiment of an exchanging method of a session key in which synchronous encryption algorithm and asynchronous encryption algorithm are mixed. 914 denotes a device for reading the card 921.

[0044] On the other hand, 913 denotes a digital camera. It is intended to record not only an operation screen image 930 of a CRT 912 but also a mug-shot of an operator, simultaneously.

[0045] This embodiment will be discussed in detail with reference to the foregoing drawings.

[0046] Concerning a procedure for detection the label, discussion will be given with reference to Figs. 1, 2 and 5.

[0047] Fig. 2 is an illustration for explaining overall construction of a system utilizing the label.

[0048] A computer 201 is connected to a network 202 having a lower security level (for example WAN), a computer 203 is connected to a network 204 having a higher security level (internal LAN) as compared with 202. A firewall 210 is present between 202 and 204. To the firewall 210, a temporary storage device 211 (for example, a magnetic disk, a flash memory) is

connected for storing the following programs, data, keys and so forth.

[0049] There is shown a manner of attaching or deleting a label 241 by the firewall 210 upon transmitting/receiving communication data from the computer 201 to the computer 203.

[0050] The firewall 210 performs process of distributing, passing and blocking and so forth of the communication data depending upon security of each communication data. Specifically, to the communication data flowing through 204, a label indicative of security is attached, and in the computer 203, access control is performed using the label. In the firewall 210, means 231 for attaching a label to communication data flowing from 202 to 204 and means 241 for deleting the label from the communication data 220 flowing from 204 to 202 stay resident.

[0051] Particularly, it is desirable to provide a label encrypting function for preventing dishonest alternation of the label 241 on the computer 203 or the network 204, electrical interception. Encrypting means 243 is cooperated with the attaching means 231 and decrypting means 242 is cooperated with revoking means 241. In the shown embodiment, an example using asymmetric encryption will be discussed hereinafter for simplification of disclosure.

[0052] The encrypting means 243 of the computer 203 and the decrypting means 242 of the firewall, and the decrypting means 233 of the computer 203 and the encrypting means 242 of the firewall are respectively corresponding encrypting and decrypting programs, respectively. Numerals 230, 240, 244 and 234 are keys to be used in encryption and decryption. A label encrypted by the public key 230 of the firewall 210 is decrypted by the private key 234 of the computer 203. A label encrypted by the public key of the computer 203 is decrypted by the private key of the firewall 210.

[0053] In the shown embodiment, it is desirable to provide a correspondence table defining a relationship among an address (such as IP address, MAC address) of a sender/receiver of information data 220, a kind (for example, port number, news, FTP, HTTP and so forth) of service, attribute information of the user ID of the sender/receiver and the label 221. By providing plural corresponding labels, it is possible to perform fine control.

[0054] In view of the system construction of Fig. 2, a flow of a content monitoring method in the computer 203 will be discussed with reference to Fig. 1.

[0055] Communication data 230 attaching the label 231 is downloaded from the firewall 210 (110). If encrypted, the label is extracted in a given format including decrypting operation (111). If the label cannot be extracted (112), error process at 140 and subsequent steps is performed. The contents of the label, such as a type indicative of security, an available range are read to make judgment whether the label is falsified one or not on the basis of digital signature given together with encryption (114). Furthermore, on the basis of the label, a security level is judged (116). Particularly, when the judgment cannot be made by a local machine, an inquiry is made to a label monitoring server (462 discussed later) on the network for retrieving a relationship between the described label and the security level (designated according to a security standard) (115, 130, 131).

[0056] When the security level can be judged and when data is judged to have a level requiring collection of history (for example, higher than or equal to a B1 level under a typical security standard TCSEC), monitoring is started (117). For example, by inputting through a keyboard, a mouse or the like, interactive operation on the screen for the downloaded communication data is performed. By performing operation

relating to transmission to an external system (such as by e-mail, FTP) or to copying on a local portable medium (for example, a magnetic disk, a hard disk), a system function defined by OS, such as calling of Winsock or File I/O in case of Windows for example, is detected (121). In the alternative, at every given period, such as every one minute (125), an image or Bitmap of the operation screen is recorded in a file (122). It should be noted that when a digital camera for picking up an image of an operator is connected to 203, the history can be recorded more effectively by recording simultaneously with the screen operation. When a program for performing operation relating to the downloaded communication data is terminated (124). If not, the process returns to step 121 (123).

[0057] Discussion will be given for error process (140, 141) relating to judgment of a security level using a label. When the label cannot be extracted or label is falsified one, an alarm indicating the contents is abusive content is displayed to a user to require judgment whether to terminal or continue (140). If the user selects "terminate", access to the downloaded communication data is terminated (141). "Continue" is selected, it is regarded that the user agreed to take operation history to advance the process to step 120.

[0058] Label extraction process 111 in Fig. 1 will be discussed in detail. Particularly, concerning circulation of content, one embodiment of encapsulation using encryption will be discussed with reference to Figs. 5 and 6.

[0059] Corresponding to the extraction process, label attaching process in the firewall 210 will be discussed.

[0060] In Fig. 6, the communication data 230 is divided into a data portion as a body of the content identified by 610 and a header portion 611 indicating attribute (serial number, content of service and so on) of the content. Adapting to such a header portion of attribute, a correspondence table 222 for

determining a label 612 to be attached (in the shown embodiment, corresponding to a keyword "Project", a label of "SECRET R&D" is adapted) is looked up by the attaching means 231. 612 is combined with 611 and 610 to be encrypted using the public key 230.

[0061] The communication data and the label thus encrypted are separated by the extracting process 111. Basically, corresponding to the attaching process, reverse process is performed. Using the private key 234, decrypting into a plain text is performed. In Fig. 5, judgment is made as to whether the encrypted communication data or not (501). As a judgment method, for example, a method for making judgment by a tag as a set of an attribute and an attribute value as defined in RFC1847 (Security Multiparts for MIME: Multipart/Signed and Multipart/Encrypted) is performed. If judged, decrypting process is attempted using the private key 234 (503). After decrypting (504), the range of a header portion (612) including the label portion is judged (505). After clipping (506), adapting to the given format of the label (507), inspection of each item (for example, security level, category) is performed (508).

[0062] Next, with reference to Fig. 3, a system construction for encrypting and collecting history 323 recorded in the primary storage device 301 at step 122 of the computer 203 will be described.

[0063] 351 denotes a computer exclusive for an auditor, 352 denotes a CRT, 353 denotes a primary storage device for accumulating the histories.

[0064] The computer 203 contains a program 311 for encrypting history 323 stored in programs 310, 311 stored in the primary storage device 301, and a program 312 for transmitting the encrypted history.

[0065] The computer 351 contains a program 361 for generating

a key and distributing the key to the computer 203, a server program 362 for collecting the histories in a hard disk 353 and a program 363 for decrypting the collected history 324 and displaying on the CRT 352. 321 and 322 are encryption keys generated by the program 361. 321 denotes a public key for encrypting a history 323, and 322 denotes a private key for decrypting the history 324. Preliminarily or in preparation for use in the encryption program 311, the key 321 is fed to the computer 203 to be stored in the primary storage device 301.

[0066] In the shown embodiment, after encryption using the public key for auditor, data is fed to a dedicated device for administrator from time to time for preventing dishonest alternation, electrical interception, wasting of disk in each computer.

[0067] Next, with reference to Fig. 4, a system construction for extracting the label attached to the content at step 130 of the computer 203 and inquiring to the server 451.

[0068] 451 denotes a computer exclusive for administrator, 452 denotes a CRT, 453 denotes a primary storage device storing a correspondence table 460 between the label and security level.

[0069] In the computer 203, a program 233 for decrypting a content 420 and a label 423 stored in a primary storage device 401, a program 412 for inspecting the label of the content, and a program 413 for performing inquiry relating to the label and encrypting the information relating to the label as it is are contained.

[0070] The computer 451 contains a program 464 generating the key and distributing the key to the computer 203, an encryption communication program 463 adapting to inquiry from the program 413, a program 462 called from 463, comparing a correspondence table 460 of the encrypted label and the security level, and

an alarming program further called from the program 462 and displaying a message of an occurrence of unauthorized security access and recording of operation history on CRT 452. On the other hand, a program 461 permitting the administrator to set the content of the correspondence table 460. 421 and 422 are encryption keys generated by the program 464. 421 denotes the public key for encryption and 422 denotes a private key for decrypting the label. Preliminarily or in preparation for use in the encryption program 413, the key 421 is fed to the computer 203 and stored in the primary storage device 401.

[0071] In the shown embodiment, meaning of security corresponding to the label may be modified by the administrator on the network depending upon the rule on the correspondence table 460.

[0072] With reference to Figs. 7 and 8, procedure of encrypted communication with the firewall 210 and the computer 203.

[0073] Fig. 7 shows processes of the encrypting program 232 in the firewall 210 and the decrypting program in the computer 203. The correspondence table 222 is provided in the firewall 210, and different encryption keys are used adapting to destination of the computer or user. Here, there is shown an example to perform encryption in the level of packet of the network (even in encryption in an application layer, similar procedure may be performed using information of user ID or the like in place of IP address or port number).

[0074] At first, security level of the network through which the content flows is judged by IP address of the sender (701). When encryption is necessary, IP address of the recipient computer 203 is extracted from the packet (702) for encrypting using the public key 230 corresponding to the IP address of the recipient (705). If the public key 230 is not present (703), encryption is performed using the public key of the firewall 210 (704). The encrypted packet is fed to the computer 203

(705). In the computer 203, when the circulated packet requires decrypting, decrypting is performed using the private key 234 corresponding to the public key 230 (712). If decryption is not possible, judgment is made that the process at step 704 was performed (713) to feed the own public key and the packet to the firewall for once decrypting the packet in the firewall, and re-encryption is performed with the public key 230 (714).

[0075] In the shown embodiment, in case of the computer not frequently performing communication with an external computer, response performance and security can be satisfied by providing re-encryption process in the firewall.

[0076] Conversely to Fig. 7, a process of a decrypting program 242 in the firewall 210 for controlling a flow of a packet from a network having a higher security to a network having a lower security, and an encryption program 243 of the computer 203 will be discussed with reference to Fig. 8.

[0077] The correspondence table 222 is provided in the firewall 210 and different decryption key is used adapting to a destination computer or user. Here, similarly to Fig. 7, there is shown an example to perform decrypting of the level of a packet in the network.

[0078] In the computer 203, judgment is made that encryption is necessary upon feeding data to other computers (801), encryption is performed by the public key adapted to the IP address of each computer (805). When judgment is made that the sender is the computer 201 belonging to a network 202 having a lower security level (803), encryption is performed with the public key 230 of the firewall 210. The encrypted communication data is transmitted as a packet (806).

[0079] In the firewall 210, IP address of the sender computer 203 is extracted from the packet, and the security level of the network through which the communication data flows, is

judged based on the IP address of the sender (811) to perform decrypting using the private key 240 of the firewall (812). If decryption is successful, the decrypted data is fed to the computer 201 in the network 202 having a lower security level from the firewall (815). If decryption failed, passing the firewall is not permitted (814).

[0080] In the shown embodiment, when data communication is performed to an external computer, decrypting into plain text is performed in the firewall to enable monitoring of taking out of security to outside.

[0081] As set forth above, the embodiment for setting the encryption key using the IP address of the computer, has been discussed. Hereinafter, another embodiment for setting the encryption key, using the user ID in the application layer, will be discussed.

[0082] Fig. 9 is a block diagram for explaining a system construction for managing the encryption key corresponding to the user ID using a portable type medium (for example, PCMCIA card 920). The computer 203 is constructed with a hard disk, a memory, a main body 911 incorporating CPU, CRT 912, a digital camera 913, a card reader 914, and a keyboard (mouse) 915. The digital camera 913 and the card reader 914 are belonging to devices of the main body 911.

[0083] On CRT 912, operation screen image 930 (multi-window) is displayed. The operation screen image 930 for operation using the keyboard 915 and the mug-shot of a user picked-up by the digital camera 913 are recorded as history.

[0084] In the card 920, a private key 923 and a public key 924 of the user, a public key 925 corresponding to the private key 940 of the firewall are incorporated. In the firewall, the public key 230 as a copy of the public key 924 and the private key 240 of the firewall are provided. For using the portable medium 920, the card reader 914 is provided. Utilizing

unspecified computers using programs 233 and 243 staying resident, convenience can be enhanced.

[0085]

[Effects of the Invention] By the present invention, problems in the prior art can be solved.

[0086] (1) Contents out of contract are not permitted to circulate.

[0087] Making reference to the label by each computer, it is made clear that copying or transferring to another system of content not attaching a proper label is not permissible to localize influence of dishonest circulation.

[0088] (2) Notifying that operation screen image being recorded as history, copying without permission by a user can be restricted.

[0089] Notification is given to a user that copy operation of the content on the computer being recorded is left as history and indicating penalty when copying without permission, violating activity can be restricted.

[0090] On the other hand, by recording an operation screen image or a mug-shot as visual history, an auditor out of organization can make judgment of non-permitted activity objectively irrespective of contents of business.

[0091] In the present invention, an auditor device exclusive for operation of an auditor as a third party, out of organization is provided on a network to transfer and accumulate operation history in each computer.

[0092] At this time, using the public key of the auditor in each computer, operation history is encrypted. The auditor decrypts the accumulated operation history using the private key stringently managed separately only in response to audit demand. As set forth, by encrypting the operation history by each computer and transferring to the audit device, it becomes possible to prevent a user or an administrator other than the

auditor from making reference to, dishonest alternation or hiding of the operation history.

[0093] In the present invention, a monitoring device dedicated for operation of an administrator in the organization is provided on a network to make judgment necessity of recording of operation history on the basis of an auditor rule table corresponding to a label.

[0094] For this reason, the administrator may control or manage access or copying of the content in each computer according to rule in the organization (domain). Maintenance operation associating with modification of rules only requires rewriting of the rule table. On the other hand, by setting of the audit rule table, it is not necessary to record all operation history for access or copying of all contents, and there is realized system operation adapting to prevention of waste of a storage medium (hard disk) accumulating the operation history and protection of privacy of the user.

[0095] In the present invention, a dedicated firewall is provided on the network to perform process of generation and disposal corresponding to input/output of communication data. In the computer belonging to the network having a higher security (for example, higher than or equal to B level of TCSEC, a function for reading the label of the communication data is provided (middle software or OS).

[0096] Therefore, the administrator may control access or copying of contents between domains having different security levels across the firewall according to the rule in the organization (domain).

[0097] Furthermore, in the dedicated firewall, labels are encrypted by the encryption key for limited people who make reference to the content. Furthermore, the decryption key which can decrypt the content is stored in the portable card (for example Smart Card, PCMCIA card) distributed per user as

session key varying the content at every communication. The decrypted content is disposed at the stage where use is completed.

[0098] Therefore, using the portable card, downloading (primary copy) of the content from the firewall to each computer is enabled whereas transferring to another system or file storage under another name (secondary copy) is restricted.

[Brief Description of the Drawings]

[Fig. 1] A flowchart of a content audit method in a computer;

[Fig. 2] A block diagram of a firewall of the present invention connecting domains having different security levels;

[Fig. 3] A block diagram of an audit device according to the present invention accumulating history of operation screen image of a terminal;

[Fig. 4] A block diagram of a monitoring device according to the present invention making judgment of necessity of recording of operation screen image of the terminal;

[Fig. 5] A flowchart showing a procedure for detecting a label in each computer;

[Fig. 6] A block diagram showing arrangement of program generating and separating the label;

[Fig. 7] A flowchart showing a procedure for decrypting communication data encrypted by the firewall in each computer;

[Fig. 8] A flowchart showing procedure for inspecting the communication data encrypted in the computer whether decrypting is possible or not in the firewall; and

[Fig. 9] A block diagram showing a construction of a computer terminal of the present embodiment.

[description of Reference Numerals]

201, 203 ... Computer

210 ... Firewall

232, 231, 241, 242 ... Program staying resident in firewall

310 ... History recording program

451 ... Administrator terminal

351 ... Auditor terminal

913 ... Camera

920 ... Card

DRAWINGS

Fig. 1

START

110 DOWNLOAD DATA

111 EXTRACT LABEL

112 LABEL CANNOT EXTRACT?

113 READ LABEL

114 LABEL FALSIFIED?

115 SERVER INQUIRY REQUIRED?

116 JUDGE SECURITY LEVEL

117 HISTORY TO BE RECORDED?

120 START MONITORING

121 COPYING OPERATION DETECTED?

122 RECORD OPERATION IMAGE

123 MONITORING END?

124 TERMINATE MONITORING

130 INQUIRE TO SERVER

131 RETRIEVE RULE

125 PER GIVEN PERIOD?

140 DISPLAY ALARM FOR NON-PERMITTED CONTENT

141 ACCESS CONTINUED?

GOAL

Fig. 2

201 COMPUTER

202 LOWER SECURITY LEVEL

231 ATTACHING MEANS

232 ENCRYPTING MEANS

233 DECRYPTING MEANS

241 REVOKING MEANS

242 DECRYPTING MEANS

243 ENCRYPTING MEANS

203 COMPUTER

204 HIGHER SECURITY LEVEL

Fig. 3

203 COMPUTER

(1) COMPUTER

310 RECORDING MEANS

311 ENCRYPTING MEANS

312 ATTACHING MEANS

361 KEY GENERATION/DISTRIBUTION MEANS

362 ACCUMULATING MEANS

363 DECRYPTING MEANS

Fig. 4

310 RECORDING MEANS

203 COMPUTER

(1) COMPUTER

233 DECRYPTING MEANS

412 INSPECTION MEANS

413 ENCRYPTING COMMUNICATION MEANS

454 ENCRYPTION KEY DISTRIBUTION

463 ENCRYPTING COMMUNICATION MEANS

462 JUDGMENT MEANS

471 ALARMING MEANS

461 RULE SETTING MEANS

Fig. 5

START

501 DETERMINE DECRYPTING PROCESS

502 DETERMINED?

503 DECRYPTING PROCESS FOR OVERALL DATA

504 CAN BE DECRYPTED?

505 CLIP HEADER PORTION

506 CLIPPED

507 CONFIRM EACH ITEM OF HEADER

508 EACH ITEM (LABEL) PRESENT?

510 CANNOT DETECTED

GOAL

Fig. 6

231 ATTACHING LABEL

610 DATA PORTION

(1) SYNTHESIZE

(2) KEY MANAGEMENT

(3) TRANSFER

230 PUBLIC KEY

234 PRIVATE KEY

232 ENCRYPTION (KEY MANAGEMENT)

650 KEY GENERATION

233 DECRYPTING

(4) SEPARATE

Fig. 7

START FIREWALL

701 ENCRYPTION NECESSARY?

702 EXTRACT COMMUNICATION DESTINATION

703 PUBLIC KEY OF COMMUNICATION DESTINATION PRESENT?

704 ENCRYPTION USING PUBLIC KEY OF FIREWALL

705 ENCRYPTION USING PUBLIC KEY OF COMMUNICATION DESTINATION

706 ENCRYPTED COMMUNICATION

GOAL

EACH COMPUTER

START

711 DECRYPTION NECESSARY?

712 DECRYPT USING PRIVATE KEY

713 DECRYPTED?

714 TRANSMIT TO FIREWALL AND RE-ENCRYPTION

GOAL

Fig. 8

START FIREWALL

801 ENCRYPTION NECESSARY?

802 EXTRACT COMMUNICATION DESTINATION

803 PUBLIC KEY OF FIREWALL PRESENT?

804 ENCRYPTION USING PUBLIC KEY OF FIREWALL

805 ENCRYPTION USING PUBLIC KEY OF COMMUNICATION DESTINATION

806 ENCRYPTED COMMUNICATION

GOAL

EACH COMPUTER

START

811 DECRYPTION NECESSARY?

812 DECRYPT USING PRIVATE KEY

813 DECRYPTED?

814 BLOCK PASSING THROUGH FIREWALL

815 TRANSMIT

GOAL

Fig. 9

914 CARD READER

210 FIREWALL

240 (PRIVATE KEY)

230 (PUBLIC KEY)

913 CAMERA

(1) USER PRIVATE KEY

925 PUBLIC KEY OF FIREWALL

915 KEYBOARD

(2) MOUSE